UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/446,583	12/22/1999	PHILIP C. LEVERIDGE	36-1302	2585

23117 7590 05/16/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SHINGLES, KRISTIE D	
ART UNIT	**PAPER NUMBER**
2141	

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/446,583	LEVERIDGE ET AL.	
	Examiner	Art Unit	
	Kristie Shingles	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-8 and 23-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-8 and 23-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant has amended claims 23 and 24.
Claims 1 and 9-22 have been cancelled.
Claims 25-43 are new.

Claims 2-8 and 23-43 are pending.

Response to Arguments

1. Applicant's arguments with respect to claims 23 and 25 have been considered but are moot in view of the new ground(s) of rejection.

Specification

2. The new title of the invention is accepted by the Examiner. The objection is therefore withdrawn.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 3, 7, 23-25, 27, 31 and 33-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bachman et al* (US 5,907,621) in view of *Carlson et al* (US 5,542,046).

a. **Referring to claim 23,** *Bachman et al* teach a method of operating an authenticating server system for authenticating a user of a client application provided on a client terminal having no unique IP address via a data communications network, the server system being arranged to control access to a document stored on a resource server connected to said data communications network, said method comprising performing the following steps in said server system:

- receiving at the resource server a request for said document generated by said client application (col.2 lines 5-8);
- evaluating at the resource server client-side persistent information accompanying said request including checking if the client-side persistent information contains an address token previously issued by the resource server which uniquely identifies the user (col.2 lines 17-19), and performing the following steps at the resource server:
- i) if no address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request: generating an address token which uniquely identifies the user, the generated address token replacing an IP address of the client terminal as a way of identifying the user (col.3 lines 34-38, col.4 lines 18-49); transmitting the generated address token to the client application in a client-side persistent information packet so that an address token which uniquely identifies the user is generated and transmitted without prior receipt at the resource server of a previously issued address token which uniquely identifies the user (col.3 lines 47-53, col.5 lines 58-63); and storing said address token for the user (col.3 lines 47-49); or
- ii) if an address token which uniquely re-identifies the user is contained in the client-side persistent information accompanying said request and the address token is an unvalidated address token: validating the address token using other authentication data received from the client terminal in said client-side persistent information and by reference to user authentication data already stored on said resource server (col.6 lines 20-37); storing the validated address token for an authenticated user and an access status of the authenticated user associated with the validated address token (col.6 lines 10-19 and 38-41, col.6 line 59-col.7 line 10); transmitting a client-side persistent information packet containing the validated address token to the client terminal (col.3 lines 47-53); or

- iii) if an address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request and the address token is a validated address token, using said validated address token to enable said resource server to validate said request for said document by checking if said stored access status for said user includes access to said document (col.6 lines 10-19 and 63-65, col.6 line 59-col.7 line 10).

Although *Bachman et al* does teach session objects wherein a session table is maintained to determine if a user's session has timed-out thus restricting user's access (col.4 lines 11-18), *Bachman et al* fail to explicitly teach validating said request for said document by checking if said stored access status for said user includes access to said document. However, *Carlson et al* teach an access status field and validating a user's access rights for accessing resources on a remote device (col.6 lines 4-6, col.7 line 50-col.8 line 28, col.8 line 66-col.10 line 42, col.11 lines 21-49). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of *Bachman et al* with *Carlson et al* by checking if said stored access status for said user includes access to said document because this step further creates another level of protection for accessing private or secure documents.

b. **Claims 25 and 43** contain limitations that are substantially equivalent to claim 23 and are therefore rejected under the same basis.

c. **Regarding claim 33,** *Bachman et al* in view of *Carlson et al* teach the method as in claim 25, *Bachman et al* further teach wherein in said server system a plurality of documents are stored on a plurality of resource servers, wherein the step of validating the authentication data of a user comprises remotely authenticating the user by reference to authentication detail of an authorized user stored by one of said plurality of resource servers, the remote authentication comprising: generating status data to distinguish said user from other users who are not currently

authenticated (col.5 lines 23-30); and generating a secret encryption key shared with said user (*Carlson et al*: col.4 lines 3-8, col.10 lines 66-67), and wherein said method of operating the authentication server further comprises: storing said status data in a storage device accessible to each of said plurality of resource servers to check an authentication status of said user by using said validated identifying tag for said client terminal received in said request (col.3 lines 25-34, col.4 lines 18-36, col.6 lines 20-37); and storing said shared secret key in a data store accessible by at least one of said resource servers for use during communications with said user (col.2 lines 17-20).

d. **Referring to claim 3,** *Bachman et al* and *Carlson et al* teach a method according to claim 23, *Bachman et al* further teach wherein said authentication step comprises receiving said address token from said client terminal with said authentication data (col.4 lines 40-49; *Carlson et al*: col.3 line 58-col.4 line 3).

e. **Claim 27** is substantially similar to claim 3 and is therefore rejected under the same basis.

f. **Referring to claim 7,** *Bachman et al* and *Carlson et al* teach a method according to claim 23, *Bachman et al* further teach timing out of said address token of a terminal of a currently authenticated user if no document request is received from said client terminal for a predetermined period (col.6 lines 10-31).

g. **Claim 31** is substantially similar to claim 7 and is therefore rejected under the same basis.

h. **Regarding claim 24,** *Bachman et al* and *Carlson et al* teach a method as claimed in claim 23, *Bachman et al* further teach wherein step (ii) further comprises: transmitting said

requested document to said client terminal along with the client-side persistent information packet containing the validated address token to the client terminal (col.3 lines 47-53; *Carlson et al*: col.7 line 53-col.8 line 28, col.9 line 20-col.10 line 42).

i. **Regarding claim 34,** *Bachman et al* and *Carlson et al* a method as claimed in claim 33, *Bachman et al* further teach wherein said authenticating step comprises issuing a challenge to the client terminal, receiving a response to said challenge, and verifying said response (col.5 lines 21-30).

j. **Regarding claim 35,** *Bachman et al* and *Carlson et al* a method as claimed in claim 33, *Bachman et al* further teach the method comprising updating said status data for an authenticated user following said storing step in said storage device (col.3 lines 25-47, col.6 lines 10-19).

k. **Regarding claim 36,** *Bachman et al* teach the method as in claim 35, wherein said updating step is performed in response to a time-out associated with said status data (col.5 lines 44-47, col.6 lines 17-19).

l. **Regarding claim 37,** *Bachman et al* teach the method as in claim 36, wherein said updating is performed in response to access by one of said resource servers to said status data (col.6 lines 20-42).

m. **Regarding claim 38,** *Bachman et al* teach the method as in claim 36, wherein said updating step is performed in response to a request by the client terminal (col.3 lines 25-47, col.4 lines 18-32, col.6 lines 10-42).

n. **Regarding claim 39,** *Bachman et al* teach the method as in claim 33, wherein said identifying tag is an IP address of the client terminal (col.4 lines 40-49).

o. **Regarding claim 40,** *Bachman et al* teach the method as in claim 33, wherein said status data is stored in a data store which each of said resource servers are able to access (col.5 line 56-col.6 line 31).

p. **Regarding claim 41,** *Bachman et al* and *Carlson et al* teach the method as in claim 33, *Carlson et al* further teach wherein said authentication details include data identifying the rights of access of individual user to one or more of said resource servers (col.6 lines 4-6, col.7 line 50-col.8 line 28, col.8 line 66-col.10 line 42, col.11 lines 21-49).

q. **Regarding claim 42,** *Bachman et al* and *Carlson et al* a method as claimed in claim 25, *Carlson et al* further teach wherein the client terminal supports a client application which the user uses to seek access to said document, and wherein the validated identifying tag comprises a unique identifying tag for the client application of the client terminal (col.3 line 58-col.4 line 3, col.6 lines 3-53; col.7 lines 50-52).

5. **Claims 4 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bachman et al* (US 5,907,621) and *Carlson et al* (US 5,542,046) in view of *Johnson et al* (US 5,560,008).

a. **Regarding claim 4,** *Bachman et al* in view of *Carlson et al* teach a method according to claim 3 as applied above, yet fail to explicitly teach wherein a new address token is issued to said client terminal if said authentication data is invalid. However, *Johnson et al* teach wherein a new address token is issued to said client terminal if said authentication data is invalid (col.13 lines 32-36). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of *Bachman et al* and *Carlson et al*

with *Johnson et al* wherein a new address token is issued to said client terminal if said authentication data is invalid because this creates a periodic re-validation of users and therefore inhibits others from masquerading as a particular user.

b. **Claim 28** is substantially similar to claim 4 and is therefore rejected under the same basis.

6. **Claims 2 and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bachman et al* (US 5,907,621) and *Carlson et al* (US 5,542,046) in view of *Kirsch* (US 5,963,915).

a. **Regarding claim 2,** *Bachman et al* in view of *Carlson et al* teach a method according to claim 23 as applied above, yet fail to explicitly teach the transmission of the address token in a cookie. However, *Kirsch* teaches that said address token is transmitted in a cookie to said user's client terminal (col.3 lines 14-16, col.13 lines 11-13). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of *Bachman et al* and *Carlson et al* with *Kirsch* by transmitting the address token in a cookie because it is a more secure manner of storage and transport of identification data.

b. **Claim 26** is substantially similar to claim 2 and is therefore rejected under the same basis.

7. **Claims 5, 6, 29 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bachman et al* (US 5,907,621) and *Carlson et al* (US 5,542,046) in view of *Johnson et al* (US 5,560,008) and further in view of *See et al* (US 6,070,243).

a. **Regarding claim 5,** *Bachman et al* and *Carlson et al* in view of *Johnson et al* teach the method according to claim 4 as applied above, yet fail to explicitly teach that the address token contains the number of times an invalid authenticator was received. *See et al* teach said address token comprises data indicating the number of times an invalid authenticator has been received from said user's client terminal (col.3 lines 23-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of *Bachman et al, Carlson et al* and *Johnson et al* with *See et al* by having the address token contain the number of times an invalid authenticator was received because a user can be denied access if they submit multiple invalid authenticators thus providing the system with added security and access control.

b. **Claim 29** is substantially similar to claim 6 and is therefore rejected under the same basis

c. **Referring to claim 6,** *Bachman et al, Carlson et al* and *Johnson et al* in view of *See et al* teach the method according to claim 5, *See et al* further teach said method comprising issuing no further address token to said client terminal if an address token received from said user's client terminal indicates that a predetermined number of invalid authenticators have been received from said user's client terminal (col.6 lines 23-26).

d. **Claim 30** is substantially similar to claim 6 and is therefore rejected under the same basis.

8. **Claims 8 and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over *Bachman et al* (US 5,907,621) and *Carlson et al* (US 5,542,046) and further in view of *Levergood et al* (US 5,708,780)..

a. **Regarding claim 8,** *Bachman et al* in view of *Carlson et al* teach the method according to claim 23 as applied above, yet fail to explicitly teach authenticating said user for access to a plurality of Web servers located in the same Internet domain. However, *Levergood et al* teach a method comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain (col.3 lines 66-67); and enabling each of said Web servers to validate document requests from the client terminal, which requests include said address token (col.3 lines 44-45), by checking said status data on receipt of a document request (col.6 lines 58-60). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of *Bachman et al* and *Carlson et al* with *Levergood et al* by authenticating said user for access to a plurality of Web servers located in the same Internet domain because this creates a more efficient system by decreasing the processing time to re-authenticate a user on multiple servers within the same domain.

b. **Claim 32** is substantially similar to claim 8 and is therefore rejected under the same basis.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: White (US 6,065,117), Miller et al (6,587,867), Bendert et al (6,275,867), Russell

(5,455,953), Ito et al (5,671,354), Dare et al (5,684,950), Tabuki (5,706,427), Gifford (5,812,776), Davis et al (6,088,805), Jones et al (5,655,077), Goldman et al (5,684,951).

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristie Shingles whose telephone number is 571-272-3888. The examiner can normally be reached on Monday-Friday 8:30-6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristie Shingles
Examiner
Art Unit 2141

kds

JASON CARDONE
SUPERVISORY PATENT EXAMINER